# Frequently Asked Questions (FAQs)

#### What is NSCAP?

NSCAP, the National Security Cyber Assistance Program, is an initiative sponsored by the National Security Agency's Information Assurance Directorate (NSA/IAD) to accredit qualified organizations to perform select cybersecurity services in support of national security system (NSS) owners and operators. By capitalizing on the industry's resources, skills, and expertise, NSCAP augments the U.S. government's ability to meet the demand. As a formal standardized program, NSCAP affirms that accredited organizations have the processes, procedures, resources, and competencies in place to deliver cybersecurity services to NSS owners and operators. NSCAP creates an exclusive and prescreened list of IAD-qualified industry partners, nationally recognized for the caliber and consistency of their cyber incident response assistance services and available to serve government, military, commercial and academic customers.

#### What is a National Security System (NSS)?

A National Security System (NSS) is any information system (including any telecommunications system) used or operated by an agency, a contractor of an agency, or other organization on behalf of an agency where the use or operation involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or is an integral part of a weapon or weapons system. This definition also encompasses systems used to support military or intelligence missions. Systems that are specifically identified within approved legislation or executive order and must be kept classified in the interest of national defense or foreign policy are also considered to be NSS. All U.S. government classified networks have been designated as NSS. (See 44 U.S.C. § 3542(b)(2), for the complete definition of "NSS".)

#### What is CIRA?

Cyber Incident Response Assistance is an identified capability under NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, Incident Response Family of Controls, IR-7 Incident Response Assistance.

By capitalizing on the industry's resources, skills, and expertise, NSCAP Cyber Incident Response Assistance (CIRA) accreditation augments the U.S. government's ability to meet the demand for incident response and intrusion detection services that NSA/IAD provides to the DOD, IC, and other organizations as authorized and directed. The core objective of CIRA accreditation is to identify companies qualified to provide rapid, on-site support to NSS owners and operators in incident response and intrusion detection. To qualify, candidate firms must demonstrate competency and expertise as identified within the CIRA Accreditation Instruction Manual.

#### Where can I find a copy of the CIRA Accreditation Instruction Manual?

The CIRA Accreditation Instruction Manual is available for download on the NSCAP web page under the heading Program Documentation.

#### Does CIRA accreditation cover all information systems used by the federal government?

The CIRA accreditation was designed to meet the growing needs of the U.S. Government, supplementing the incident response and intrusion detection services that NSA/IAD provides to the DOD, IC, and other organizations as authorized and directed. CIRA accreditation is awarded to qualified CIRA providers who are capable of providing comprehensive CIRA services to operators of classified and unclassified national security systems. (See What is a National Security System?)

#### Who may apply for NSCAP CIRA accreditation?

Any U.S. organization that offers CIRA services as a core part of its business model. Broadly speaking, assessment of capabilities is based on the provider's ability to:

Consistently deliver services using repeatable processes and procedures.

- Assign highly skilled and qualified staff, who are eligible to hold U.S. Government Security clearances, to follow outlined processes and procedures to deliver services.
- Maintain and improve the quality of delivered services through training initiatives, improvement of analytical capabilities, and use of lessons learned from previous deployments or engagements to refine processes.

### Is the accreditation available within NSA? Are private sector companies competing against internal NSA teams?

No. Commercial entities may apply for NSCAP accreditation to supplement NSA incident response activities in support of all NSS owners. The NSCAP accreditation is designed to encourage a partnership between commercial CIRA service providers and NSA. Accredited companies are also free to provide CIRA services to government, military, commercial and academic customers.

#### Is there an application fee?

Candidate organizations **are not charged any fee** for applying for accreditation. Additionally, the NSA/IAD **will not** fund any portion of the costs incurred by an applicant/ candidate Organization to work through the accreditation process or, once accredited, to maintain accreditation status.

#### Is there any restriction as to the size of the company that may apply for accreditation?

No. It is expected that each candidate organization will utilize at least one "Core Team" as part of its overall CIRA service offering. Each core team must consist of at least five different key team members. With the submittal of its application package, the candidate organization corroborates that the skills of five different key team members identified and listed in Appendix C, Section 3 – CIRA Key Team Qualifications Report meet the specialized expertise requirements for each key team member specialization as shown in Appendix B, Table 2: CIRA Key Team Qualifications Guidance in the CIRA Accreditation Instruction Manual.

#### Can a person on the core team be dual-hatted? Are five unique people required or is it five capabilities?

Yes. A person can be dual-hatted per operational engagement; however, for the purpose of NSCAP CIRA Accreditation, there must be 5 unique individuals on the key staff team with the requisite skills that respond to the criteria indicated in Appendix B, Table 2: CIRA Key Team Qualifications Guidance in the CIRA Accreditation Instruction Manual.

# Our organization provides incident response assistance services under a Managed Security Services model where services are provided through remote monitoring. Is this model acceptable for earning an accreditation?

CIRA accreditation is for on-site incident response services that include intrusion detection, malware analysis and reverse engineering, forensics, packet capture (PCAP) and network traffic analysis, host integrity checking, containment, eradication, remediation, and on-going mitigations. Additionally, there are expectations that the candidate organization will be fully positioned to provide these services when needed and that the provisioning of these services is not dependent on the client purchasing some other service or product from the candidate. As NSS owners and operators may not be able to move data and information to remote locations for analysis and support, the work needs to be performed on site. This answer also applies to outsourcers that provide incident response assistance services as part of their outsourcing service offering.

## What is the NSCAP accreditation process?

The candidate organization will assemble a complete application package as outlined in Appendix C of the CIRA Accreditation Instruction Manual available on the NSCAP website. Upon submission to the NSCAP Office, the application package is evaluated to determine if the accreditation criteria are met, then it is scored accordingly. If a passing score of 85% or more is achieved, the candidate organization will be accredited. The organization then receives a formal letter and certificate of accreditation valid for 24 months.

#### How do I submit my organization's application package?

Applications for CIRA accreditation are submitted through the new NSCAP Accreditation Portal (NAP) using the 4 quick steps below:

- 1. Use the following link to access the NAP homepage: https://www.iad.gov/Cira/login\_join.cfm
- 2. Click the **New Registration** button to fill in the form to first register your organization.

- 3. Use the link in your registration acknowledgment email to return to the NAP home page and use the **New Registration** button to create your new account username and password.
- 4. Once you receive an email that your account is approved, return to the NAP homepage, enter your username and password in the Login block and begin your application.

#### How long does the NSCAP accreditation process take?

The Government's goal is to complete the accreditation process within 60 days as application packages are received from a candidate organization.

#### If accredited, how will my organization be contacted to perform services?

Your organization's contact information will be added to the list of CIRA-accredited organizations on the NSCAP web page. NSS owners and operators may use the list of accredited service providers at any time.

#### How long is the accreditation valid?

The CIRA accreditation is valid for 24 months.

#### Are accredited organizations allowed to subcontract?

Yes. However, an accreditation awarded to an organization does not imply or bestow that same accreditation to the subcontractor individual or partner. Therefore, the organization seeking accreditation must retain the services of employees with the credentials and experience to satisfy the accreditation criteria. See Appendix B – CIRA Key Team Qualifications Guide in the CIRA Accreditation Instruction Manual. Part-time contractors, subcontractors and other resources may be part of the organization's CIRA team. However, any individual certifications and qualifications from other organizations may not be counted toward this accreditation.

#### Do you expect that in the future NSCAP accreditation will be required to provide CIRA services to NSS systems?

Yes. Our current expectation is that NSCAP accreditation will be required of any company seeking to do business with the NSS community.

#### What is required for accreditation renewal?

Renewals are not automatic. If an accredited organization wishes to renew its accreditation, it must submit it renewal application to NSA/IAD no later than 30 days before the end of the accreditation period. Renewals are voluntary, but require the timely submission of a Renewal Application Package to be submitted to NSA/IAD through the application process.

The Renewal Application Package must include the following:

- 1. It is required that the accredited organization provide confirmation that providing CIRA services remains a focus of their business model. The statement must be signed by two executive officers from the Accredited Organization who have the authority to make this level of commitment.
- 2. It is required that the accredited organization provide past performance reports in the format required by Section 6.6 Past Performance, covering any additional work performed during the previous 24 months. NSA/IAD expects that the accredited organization will have performed at least three CIRA service engagements during that reporting period. Any NSS CIRA service engagement that was performed during the period of past performance should be included as part of the Renewal Application Package.
- 3. If applicable, the accredited organization must report and provide copies of any updates, enhancements or replacements to their processes and procedures that were changed from those accepted as part of their initial accreditation or accepted in subsequent renewal submittals.
- 4. If applicable, the accredited organization must report staffing changes to its Key Team Members and provide an updated CIRA Key Team Qualifications Report as part of its Renewal Application Package.
- 5. The previously accredited organization is responsible for identifying and complying with all accreditation requirements included in the version of the manual posted at the time of their renewal application. If applicable, the accredited organization must report and submit any other changes to any components that were originally contained in the Application Package or in subsequent renewal application packages, or to make their renewal package compliant with the current version of the manual that is in use at the time of application for accreditation renewal.

If no changes were made to the documents identified in items 3-5 within this list during the renewal period, the accredited organization must provide a statement to NSA/IAD with their renewal submittal that no changes were made. The Accredited Organization will assemble the appropriate content for inclusion in the Renewal Application Package and provide the package to NSA/IAD through the submittal process. All content provided as part of this Renewal Application Package must be identified as renewal content.